

AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims

1. (Currently Amended) A network ~~Network~~ comprising at least one access point (~~AP1, AP2~~) and one access controlling node (~~WSN, AS~~), the access points making use of the IAPP protocol for inter AP communication, wherein at least one station (~~STA1~~) may associate with the access points (~~AP1, AP2~~), whereby the identity of the station can be approved by the access controlling node (~~AS~~), wherein:

the access controlling node (~~AS~~) ~~[[is]]~~ monitors whether a given station is having access to any of a given subset of access points and monitors an account relating to the given station being associated with a given access point of the subset of access points~~[[,]]~~; and,

if detecting that the account relating to the given station is zero or if the user of the station has been idle for a given length of time,

the at least one access-controlling node (~~AS; WSN~~) issues at least one IAPP message causing the AP of the subset with which the station is currently associated to disassociate the given station, and thereby terminating access for the given station.

2. (Currently Amended) The network ~~Network~~ according to claim 1, wherein a first access-controlling node (~~AS; WSN~~) is an authentication server connected to the Internet.

3. (Currently Amended) The network ~~Network~~ according to claim 2, wherein a second access control node is provided, the second access control node being a gateway node (~~WSN~~).

4. (Currently Amended) The network ~~Network~~ according to claim 2, wherein the access-controlling node issues an IAPP ADD notify message.

5. (Currently Amended) The network ~~Network~~ according to claim 2, wherein the access-controlling node issues an IAPP move notify message.

6. (Currently Amended) The network ~~Network~~ according to claim 3, wherein the access-controlling node issues a Lock out request (103) to the gateway node.

7. (Currently Amended) An access ~~Access~~ controlling node connecting to at least a group of access points, the access points making use of the IAPP protocol for inter AP communication and providing access to at least one station (STA4), ~~the station (STA4),~~ whereby the identity of the station can be approved by the access controlling node (AS), ~~whereby~~ wherein:

the access controlling node (AS) ~~[[is]]~~ monitors whether a given station is having access to any of a given subset of access points and monitors an account relating to the given station being associated with a given access point of the subset of access points~~[[.]]~~; and,

if detecting that the account relating to the given station is zero or if the user of the station has been idle for a given length of time,

the at least one access-controlling node ~~(AS; WSN)~~ issues at least one IAPP message causing the AP of the subset with which the station is currently associated to disassociate the given station, ~~and~~ thereby terminating access for the given station.

8. (Currently Amended) A method ~~Method~~ of terminating access for a WLAN station comprising the steps of:

monitoring whether a given station is having access to any of a given subset of access points and monitoring an account relating to the given station being associated with a given access point of the subset of access points~~[[.]]~~ and,

if detecting that the account relating to the given station is zero or if the user of the station has been idle for a given length of time,

issuing an IAPP message causing the access point of the subset with which the given station is associated to disassociate the given station.